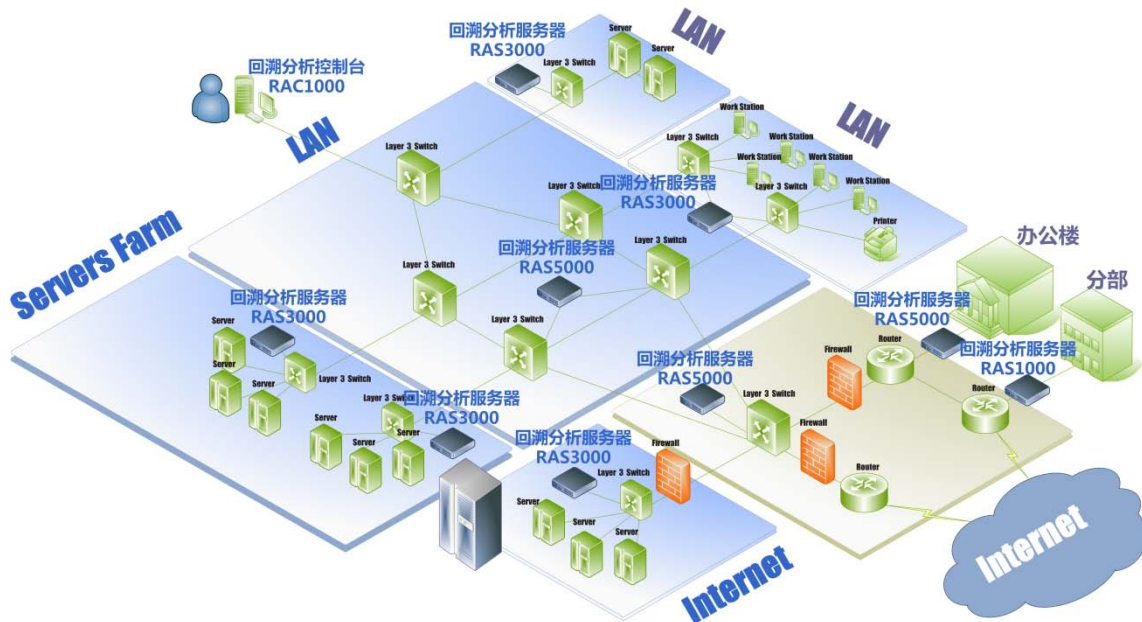


科来网络回溯分析系统

科来网络回溯分析系统是能够长时间记录网络通讯数据，并提供基于时间的数据挖掘分析系统。



产品优势：

7X24 小时的关键网络通讯数据的实时分析与收集保存

通过长期捕获关键网络的网络通讯数据，实时分析并分类记录所有的网络用户的网络行为数据，网络通讯数据和应用访问数据，从而为网络问题分析、网络行为分析、网络性能和应用性能分析提供最完整，最有力的数据基础。



基于时间的网络通讯数据回溯分析

能够快速追溯到任意时间范围内的重点分析目标的通讯数据，包括与其关联的通讯数据的快速挖掘和全面分析，帮助用户快速定位分析网络和应用问题，发现和攻击安全攻击，对网络用户的网络行为进行深入有效的高精度分析。

功能特点：

高性能的数据捕获和存储

千兆性能的网络流量实时处理能力，能够线速的保存骨干链路上的所有通讯数据，包括所有的数据流信息和数据包。

长期的数据保存能力

集成的大容量存储系统，可提供从 500GB 至 63TB 的专用网络回溯分析系统硬件，同时可根据用户的需求提供更大容量存储系统的定制硬件，提供关键链路网络通讯数据的长期存储。

高效快速的数据挖掘和检索

提供任意时间范围的网络通讯数据挖掘能力，能够快速检索到主机、应用的通讯信息，同时对数据流信息进行检索和挖掘，直到相关数据包快速挖掘，帮助用户快速定位挖掘特定分析目标的网络通讯数据。

全面深入的网络通讯分析能力

提供科来网络分析系统的对网络通讯的各种全面深入分析功能，包括强大的专家系统智能分析、数据包详细解码分析、节点分析、数据流分析、安全分析、应用层日志分析等对网络通讯的多种精细分析能力。

技术优势：

数据包的回溯分析对各种网络和安全问题提供强有力的分析取证能力。

专用的软硬件一体化设计，安装部署容易，支持远程部署，远程访问，支持对分布在不同地点的多条网络链路通讯进行集中长期监控分析。

方便高效的数据检索和数据挖掘界面，提供直观高效的数据分析和挖掘能力，业界领先的逐级数据挖掘分析视图，可根据时间、主机、应用、会话进行逐级数据挖掘，方便高效的挖掘所需分析数据。

支持方便快捷的数据导出能力，能够提供多种格式的数据包文件，并支持数据包播放功能，方便其他分析系统进行数据分析。

专用的文件存储格式和方式，其他程序无法直接访问读取回溯服务器保存的网络通讯数据，同时提供用户访问认证和授权控制功能，保证系统数据的安全性。

采用 RAID5 和 RAID6 存储技术，保证存储数据的可靠性。

硬件规格：

回溯分析服务器 RAS1000 系列

回溯入门级系列，针对出口在 100M 带宽的网络，提供 500GB 的数据存储。采用 RAID1 存储，保障数据安全。



回溯分析服务器 RAS3000 系列

高性价比产品系列，针对中型网络，采用 RAID5/RAID6 存储技术，存储容量最高可达 21TB，冗余电源，可热插拔驱动器，并支持 8 口千兆以太网链接。



回溯分析服务器 RAS5000 系列

中高端产品系列，针对更大规模网络，采用 RAID5/RAID6 存储技术，存储容量最高可达 42TB，冗余电源，可热插拔驱动器，并支持 8 口千兆或 2 口万兆以太网链接。

